

Claims

1. A system for providing a user (10) an authority to a secure domain (70, 80) in a network for data or telecommunication, comprising:
 - an interface to the user (10), requiring the authority through at least one access code;
 - 5 an authenticating server (20), for authenticating user-certificate data and user-identification data corresponding to said access code;
 - an access server (60), for providing at least one access key pair if at least one of the identification data and certificate data is authenticated;
 - 10 said access server (60) having said access key pair stored in at least one user deposit module (50);
 - said access server (60) providing said access key pair to said interface; and
 - whereby said access key pair directly provides the authenticated user (10) the authority to enter said domain (70, 80) through a server access independent signal path (100, 110).
- 15 2. A system according to claim 1, furthermore comprising means for checking access privilege-level data for the authenticated user.
3. A system according to one of claims 1-2, wherein the access key pair is arranged to directly access the authenticated user to the parts of the secure domain (70, 80) corresponding to a user-level of privilege, thus enabling an on-line real-time provision of applications and services according to a preset level of priority, access or security requirements for domain entry for the authorised user (10).
- 20 4. A system according to one of claims 1-2, wherein the access key pair is arranged to enable the user to encrypt, digitally sign and authenticate data relevant to the secure domain (70, 80) in correspondence to a user-level of privilege, thus enabling an on-line provision of cryptographic measures according to a preset level of priority, access or security requirements in the security domain in real-time.
- 25 5. A system according to one of claims 1-4, wherein the access server (60) is arranged to provide and store at least one new access key pair for each user-attempt to access the secure domain (70, 80), allowing a user (10) only one access attempt to a domain (70, 80) with the same access key pair.
- 30 6. A system according to one of claims 1-4, wherein the access server (60) is arranged to provide at least one previously stored access key pair for additional authority-requests to the domain (70, 80) following an initial domain authorization.

7. A system according to one of claims 1-6, wherein the access key pair is comprised in a virtual smart card.

8. A system according to one of claims 1-6, wherein at least three access key pairs are provided and stored in the user deposit module via the access server (60), a first key pair for authentication purposes, a second key pair for encryption purposes and a third key pair for digital signing purposes.

9. A system according to claim 8, wherein the at least three access key pairs are comprised in a virtual smart card.

10. A system according to one of claims 1-9, having an interface to an authority (30) for validating user-credentials.

11. A system according to one of claims 2-10, wherein the user-level of privilege is determined by stored privilege level data for the user (10).

12. A system according to one of claims 2-11, wherein the user-level of privilege is determined by the user certificate data and user identification data.

15 13. A system according to one of claims 2-12, wherein the user-level of privilege is determined by at least one of priority-, access- and security level data for domain entry.

14. A method for providing a user (10) an authority to a secure domain (70, 80) in a network for data or telecommunication, comprising the method steps of:

requiring the authority via a user-interface, through at least one access code;

20 authenticating user-certificate data and user-identification data corresponding to said access code;

providing at least one access key pair via an access server (60), if at least one of the identification data and certificate data is authenticated;

having said access key pair stored in at least one user deposit module (50);

25 providing said access key pair to said interface; and

whereby said access key pair directly provides the authenticated user (10) the authority to enter said domain (70, 80) through a server access independent signal path (100, 110).

30 15. A method according to claim 14, wherein access privilege-level data is checked for the authenticated user.

16. A method according to one of claims 14-15, wherein the access key pair directly accesses the authenticated user to the parts of the secure domain (70, 80) corresponding to the user-level of privilege, thus enabling an on-line real-time provision of applications and

services according to a preset level of priority, access or security requirements for domain entry for the authorised user (10).

17. A method according to one of claims 14-15, wherein the access key pair enables the user to encrypt, digitally sign and authenticate data relevant to the secure domain (70, 80) in correspondence to a user-level of privilege, thus enabling an on-line provision of cryptographic measures according to a preset level of priority, access or security requirements in the secure domain in real-time.

5 18. A method according to one of claims 14-17, wherein an access server (60) provides and stores at least one new access key pair for each user-attempt to access the secure
10 domain (70, 80), allowing a user (10) only one access attempt to a domain with the same access key pair.

15 19. A method according to one of claims 14-17, wherein an access server (60) provides at least one previously stored access key pair for additional authority-requests to the domain (70, 80) following an initial domain authorization.

20 20. A method according to one of claims 14-19, wherein the access key pair is comprised in a virtual smart card.

25 21. A method according to one of claims 14-19, wherein at least three access key pairs are provided and stored in the user deposit module via the access server (60), a first key pair for authentication purposes, a second key pair for encryption purposes and a third key pair for digital signing purposes.

22. A method according claim 21, wherein the at least three access key pairs are comprised in a virtual smart card.

23. A method according to one of claims 14-22, wherein user-credentials are validated via an interface (30) to an authority.

25 24. A method according to one of claims 14-23, wherein the user-level of privilege is determined by stored privilege level data for the user (10).

25 25. A method according to one of claims 14-23, wherein the user-level of privilege is determined by the user-certificate data and user-identification data.

30 26. A method according to one of claims 14-23, wherein the user-level of privilege is determined by at least one of priority-, access- and security level data for domain entry.
